Principles of Cryptography Problem Sheet 3

Dr. Kurunandan Jain[1]†,

[1]Department of Mathematics, Amrita Vishwa, Amrita Campus, Kollam-690525, Kerala, India

(Received xx; revised xx; accepted xx)

1) As we have seen in class, public key cryptography can be used for encryption and key exchange. Furthermore, it has some properties which are not offered by secret key cryptography

So why do we still use symmetric cryptography in current applications?

2) Assume a small company with 120 employees. A new security policy demands encrypted messages exchange with a symmetric cipher. How many keys are required if you are to ensure a secret communication for every possible pair of communicating parties?

3) Compute the gcd of 7469 and 2464

b) Compute gcd of 2689 and 4001

4) Using the extended Euclidean algorithm, compute the greatest common divisor and the parameters s and t of

a) 198 and 243

b) 1819 and 3587

5) Find the inverses of $a = 7$ and $m = 26$

b) $a = 19$ and $m = 999$

5) Determine $\phi(m)$ for $m = 12, 15, 26$ using the definition and check for each integer $gcd(n, m) = 1$

6) Compute the inverses of a modulo n

a) $a = 4$ and $n = 7$

b) $a = 5$ and $n = 12$

c) $a = 6$, $n = 13$

7) Verify Euler's Theorem holds in $\mathbb{Z}_m$ for $m = 6, 9$ for all the elements a for which $gcd(a, m) = 1$. Also verify that the theorem does not hold for all elements a for which $gcd(a, m) \leqslant 1$.

8) Let the two primes $p = 41$ and $q = 17$ be given as a set-up parameters for RSA

a) Which of the parameters $e = 31$ and $e = 49$ are a valid RSA exponent?

b) Compute the public and private keys, showing every step of the calculation

9) Applying the square and multiply algorithm calculate

a) $x = 2$, $e = 79$, $m = 101$

b) $x = 3$, $e = 197$ and $m = 101$

10) Using RSA and the parameters encrypt the message

a) $p = 3$, $q = 11$, $d = 7$, $x = 5$

b) $p = 5$, $q = 11$, $e = 3$, $x = 9$

11) In practice the short exponents $e = 3, 17$ and $e = 2^{16} + 1$ are widely used

a) Why can't we use these three exponents as values for d in applications where we want to accelerate decryption?

12)

† Email address for correspondence: kurunandanj@am.amrita.edu